2018-08-13

Technology Innovation is Great but Strategy is Better

Blanken, Leo; Davis, Zachary

Technology Innovation Is Great, But Strategy Is Better

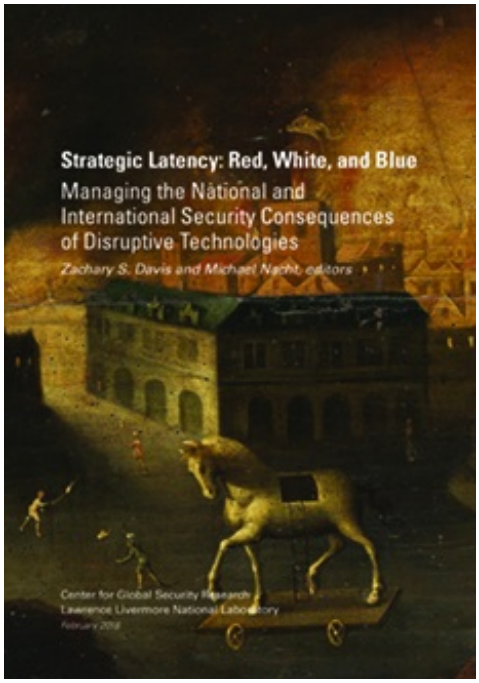
thestrategybridge.org/the-bridge/2018/8/13/technology-innovation-is-great-but-strategy-is-better

Strategy Bridge

August 13, 2018

Leo Blanken and Zachary Davis

This article is part of a new series on The Strategy Bridge *analyzing some of the issues surrounding the problem of #TechnologyInnovation.*



The Strategic Latency Project—based out of Lawrence Livermore National Laboratory's Center for Global Security Research—explored the impact of changing technology on U.S. national security. The term *strategic latency* refers to the potential of emerging commercial technologies to shape or disrupt the international security landscape. The project brought together researchers from the academic, applied science, military, and commercial realms to tackle this issue and produce a useful construct for framing the debates, as well as to generate some tentative conclusions. The result was an organizing scheme of three lenses: *Red* (referring to technology's potential to empower enemies), *White* (referring to the nature of the commercial technology space), and *Blue* (referring to technology's potential to empower the U.S. and its allies). The key conclusion of this project, contained in the report entitled *Strategic Latency: Red, White, and Blue* edited by Zachary Davis and Michael Nacht, was that the roles of strategy, culture, and institutional change are the keys to understanding the interface of commercial technology and national security. In other words, rapidly changing technologies are important, but they have strategic implications only when understood within the context of the human actors and institutions that give them meaning and purpose.

Much ink has been spilled recently about the potential strategic impact of technology sectors such as cyber tools, gene editing, nanotechnology, artificial intelligence, and other advancements. Elon Musk recently told the South by Southwest conference, "The danger of [artificial intelligence]is much greater than the danger of nuclear warheads by a lot…" Stephen Hawking told *Wired* in 2017, "I fear that [artificial intelligence]may replace humans altogether." Even national security elites do not seem to be immune; in his 2016 threat

assessment, the Director of National Intelligence pronounced the CRISPR—short for Clustered Regularly Interspaced Short Palindromic Repeats—gene editing technology to have become a weapon of mass destruction. Taken at face value, these pronouncements implies a number of technology-driven revolutions are going to take the international security landscape by storm, and the U.S. military needs to be prepared.

From the advent of interchangeable-part manufacturing at the Springfield Armory, to aviation, to the global positioning system (GPS), the military took the lead in driving America's technological landscape.

Is the strategic landscape going to be disrupted? If so, why does the U.S. national security apparatus appear to be so befuddled? One reason is that, for most of American history, the core driver of technology *was* the national security apparatus; it provided the funding for basic and applied research as well as the engineering to turn good ideas into working technology. From the advent of interchangeable-part manufacturing at the Springfield Armory, to aviation, to the global positioning system (GPS), the military took the lead in driving America's technological landscape. Further, these trailblazing efforts buoyed the private sector by pushing foundational technologies such as computers and the internet to the point where private firms could build follow-on innovations without bearing the burden of massive initial investments in research and development.

Artist's conception of GPS Block II-F satellite in Earth orbit. (NASA/Wikimedia)

In other words, the defense establishment has traditionally been the pioneer in conceiving and developing radical technological advancements, while the private sector enjoyed the benefits. Some argue this dynamic has changed in recent years, leaving the military behind in the technology race. The title of a recent academic article sums this trend up: "U.S. R&D at All-Time High, Federal Share Reaches Record Low." These investment trends help to explain the current debate on technology and provided the impetus for the Strategic Latency Project. By looking at technology through the lenses of *Red*, *White*, and *Blue* the contributors could parse out the dynamics of these issues in the newly emerging innovation landscape.

...the discussion around the threat side of technology should focus more on the goals and nature of adversaries than on the physical potentialities of technology.

In regards to the threat (*Red*) aspect of emerging technology, the Strategic Latency Project shows deep analyses are needed to link technological potential to realized capability. On the one hand, current discussion around new technology tend to be speculative, focused on what actors *could* do if they combine the intent and capability to weaponize scientific advancements in various fields. C. Wes Spain's chapter of the Strategic Latency report, for example, shows man-portable air defense systems (MANPADS) represents a "dog that did not bark"—a technology that was hyped as a game-changer and failed to materialize as such. His work points out the gap between technological potential and operational reality. Celeste Chen, Jacob Andriola, and James Giordano's chapter, on the other hand, traces a concerted effort on the part of the Chinese government to build a deep latent potential in neuroscience and biotechnology capabilities that shows all of the signs of marking a true potential shift in the strategic balance on the international stage. Jennifer Snow's chapter on additive manufacturing (AM) shows that such analyses should involve the participation of a wider range of voices—to include makers, hackers, and other underlying communities that exist on the bleeding edge of such technology. In sum, the discussion around the threat (*Red*) side of technology should focus more on the goals and nature of adversaries than on the physical potentialities of technology.

Where have all the MANPADS gone? (Wired)

Taken as whole, the work of these authors exemplifies how analyses of strategic latency can be done. Scenarios focused on the attributes of technology are useful thought experiments but should not be the basis for policy decisions. Instead, better cross-pollination of expertise

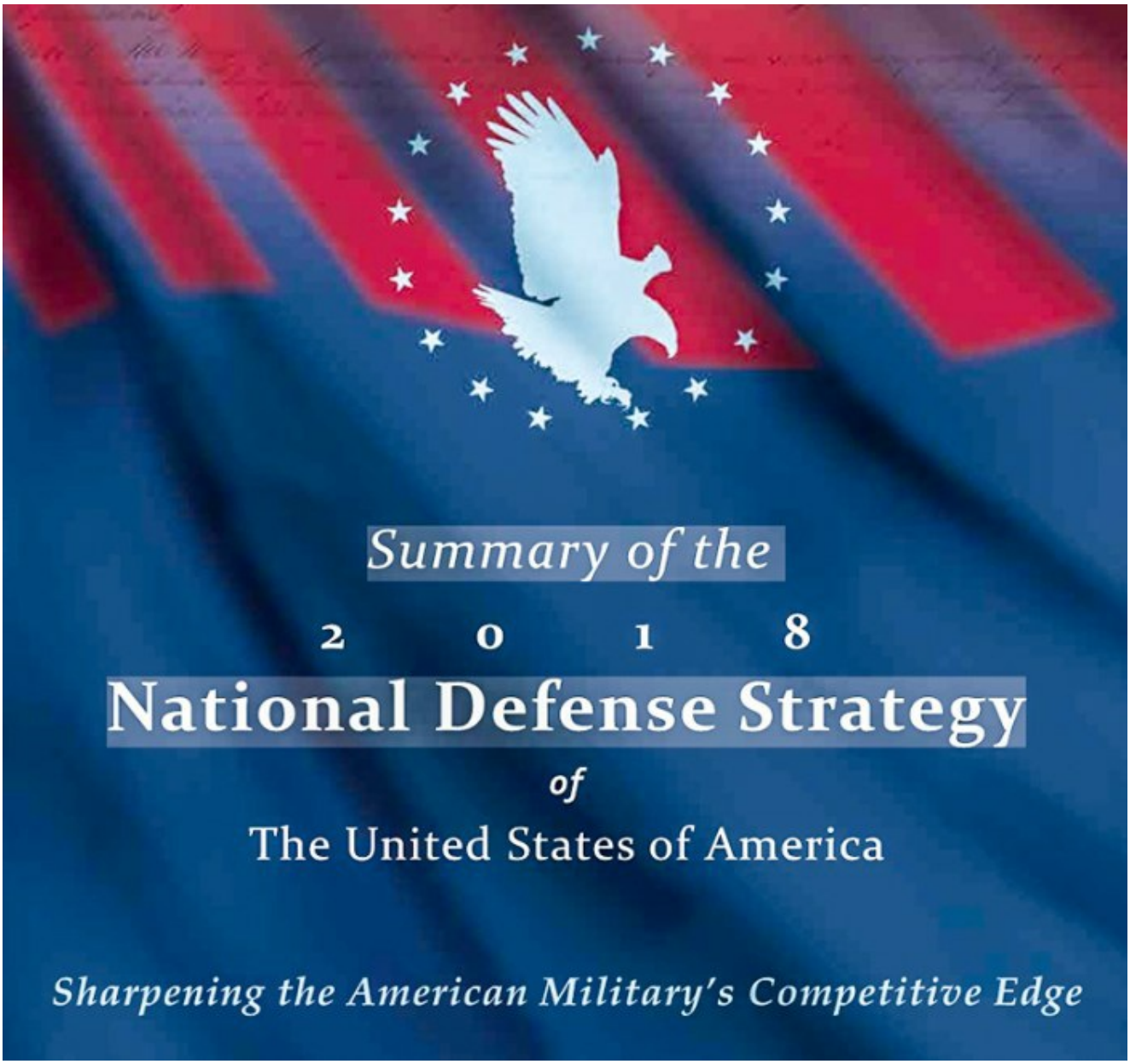
—including tech-nerds, sober policy experts, and seasoned operators—is essential. These perspectives must be balanced to uncover the likely impact of today's emerging technology.

The Project's authors take a wide range of positions on the nature and importance of current technological trends (*White*). Paul Bracken argues there is a democratizing nature to today's rapidly changing technologies. In other words, lower barriers to entry for emerging strategic technologies will serve to level the playing field among states and reduce the capacity of superpowers to manage the international system. Others in the Project disagree. David Chu, for example, argues that current technology may not be evolving all that rapidly, given a broader view of history. If this is true, it may be the case that existing planning and programming mechanisms in countries such as the United States should be able to contend with new technologies as they emerge. Leo Blanken and Jason Lepore model an optimal technology investment strategy within these changing conditions, and find that vibrant emerging tech sectors may be a serious liability for nations unable to effectively leverage their own technology ecosystem. Taken as a whole, these chapters show that it is unclear how *radical* current technology trends are, and that government understanding of these trends is very poor. To narrow this gap, more effort must be made by governmental actors to understand the culture and dynamics of the commercial white space. This would go beyond haggling over acquisition reform and funding mechanisms, but would involve a genuine and sustained discussion of the shared interests and concerns of both sets of actors.

...the U.S. government should resist the urge to "become more like Silicon Valley," but rather alter its own cultural lens to better exploit private sector innovations.

For the U.S. national security apparatus (*Blue*) to best leverage emerging technology, authors of the Project converge on the common theme of the importance of maintaining a robust innovation base, constituted by a healthy research and development pipeline complemented by public-private partnerships capable of rapid response. New entities—such as the Defense Innovation Unit Experimental (DIUx, recently renamed, dropping the "experimental" moniker to reflect its normalization within the Department of Defense), the Special Capabilities Office (SCO), and Special Operations Command's SOFWERX—join established government innovation hubs such as the Defense Advanced Research Projects Agency (DARPA), the national laboratories, and Central Intelligence Agency's In-Q-Tel investment fund in the effort to keep American spies and warfighters armed with cutting-edge technology. Frank Gac, Timothy Grayson, and Joseph Keogh map the range of public-private partnership models and conclude that some of the key challenges include creating agile funding mechanisms and integrating emerging technologies with legacy systems and platforms. Toby Redshaw makes the powerful case that the U.S. government should resist the urge to "become more like Silicon Valley," but rather alter its own cultural lens to better

exploit private sector innovations. Brian Holmes focuses on the purpose of technology acquisition—developing the best mix of weapons for the disruptive future combat environment. To do so, he argues, will require fresh strategic thinking that moves beyond the expensive gold-plated platforms of the Cold War. The consensus of these chapters is that the challenge for *Blue* in the emerging technology environment moves beyond bureaucratic tweaks and increased spending. This new climate will necessitate a shift in mindset—a changing of the culture and strategic lens of American security institutions to effectively leverage the commercial technology space.



The Strategic Latency Project shows that understanding people and institutions is crucial for getting things right. Pursuing technology for technology's sake is a real risk that can deplete the Pentagon's coffers and potentially aid enemies who reap the fast follower rewards in an era of rapid technology development and diffusion. What is needed to guide technology

innovation efforts is a strategy that links foreign policy goals to deployable technologies. Consider the recently released National Defense Strategy; while it provides some clarity on what capabilities are likely to be relevant for the emerging near-peer threat environment, it is light on the trade-offs needed to prioritize technology acquisition policies. For example, the technologies required by U.S. forces for counterterrorism may be very different from those needed for great power conflict, countering weapons of mass destruction, or space warfare. With limited resources, hard choices are mandatory. What's missing is a strategy that accounts for latent and emerging technology-enabled threats and matches them with prioritized military requirements. Such a strategy would include an optimized mix of new and old technologies designed to exploit adversary vulnerabilities and minimize American weaknesses. There is reason for optimism in America's potential to leverage technology for its own security as long as leaders make the hard choices around national priorities that will allow planners and strategists to engage technology with focus and purpose.

Leo Blanken is an associate professor in the Defense Analysis Department of the Naval Postgraduate School. He is the author of Rational Empires: Institutional Incentives and Imperial Expansion *and co-editor of* Assessing War: The Challenge of Measuring Success and Failure*.*

Dr. Zachary Davis is Senior Fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory and a Research Professor at the Naval Postgraduate School. He is editor of The Proliferation Puzzle: Why States Proliferate and What Results *and* The India-Pakistan Military Standoff: Crisis and Escalation in South Asia*.*

The views expressed here do not represent those of the Naval Postgraduate School, the U.S. Navy, Department of Defense, or any part of the U.S. government.

Have a response or an idea for your own article? Follow the logo below, and you too can contribute to The Bridge:

Enjoy what you just read? Please help spread the word to new readers by sharing it on social media.

Header Image: Strategy Guides Technological Innovation (CalvinAyre.com)